Federal Public Key Infrastructure Policy Authority (FPKIPA)

Minutes of the 9 August 2005 Meeting

GSA; 1800 F Street; Room 5141A; Washington, DC

A. AGENDA

1) Welcome & Opening Remarks / Introductions
2) Discussion / Vote on Minutes from 12 July meeting
3) Electronic Mail Votes
4) Discussion/Vote on Draft Bylaws Document
5) Discussion of Audit Cycle Review Issues
6) Discussion: New FBCA Policy Update – NO VOTE
7) FPKI Certificate Policy Working Group (CPWG) Reports
    a. Discuss mapping DoD in 3647 Format
    b. Discuss Common Policy High Assurance Level Policy
    c. Vote to Map Boeing at Medium Assurance Level
8) FPKI Operational Authority (FPKI OA) Report
    a. Requirement for maintenance of test environments
    b. Status of FBCA/Applicant Cross-Certification Technical Testing
9) Other Topics
10) Adjourn Meeting

B. ATTENDANCE LIST

VOTING MEMBERS

The meeting started with 10 members (a quorum is 9).

Organization	Name	Email	Telephone
Department of Commerce (NIST)	Polk, Tim		
Department of Defense	Hanko, Dave		
Department of Energy	Breland, Mary Ann		
Department of Health & Human Services	Alterman, Peter		
Department of Homeland Security	Absent		
Department of Justice	Morrison, Scott		
Department of State	Caldwell, Sally		
Department of the Treasury	Moldenhauer, Michelle		
GSA	Cornell, John		
NASA	DeYoung, Tice		
OMB	Absent		
USDA/NFC	Goodwin, Linda/Lewis Collins		
USPTO	Purcell, Art		

ACTION: Dr. Peter Alterman will discuss with Ms. Jeanette Thornton the possibility of OMB becoming an ex officio member of the FPKIPA. This action was the result of a suggestion by Dr. Tice

DeYoung that OMB be made an ex-officio member of the FPKIPA. There was a general consensus of the group that this was a good idea.

OBSERVERS

Organization	Name	Email	Telephone
FPKI OA (Mitretek)	Stern, Michael		
Department of State (ManTech)	Froehlich, Charles R.		
Department of the Treasury (eValid8)	Dilley, Brian		
FPKI OA Program Manager	Jenkins, Cheryl		
FICC Support (FC Business Systems)	Petrick, Brant		

C. MEETING ACTIVITY

Agenda Items 1 & 2

Welcome & Opening Remarks / Introductions **Dr. Peter Alterman**
Discussion / Vote on Minutes from 12 July meeting **Mr. Brant Petrick**

This meeting took place at the GSA Central Office Building, 1800 F Street, Washington, DC in Room 5141A. Dr. Peter Alterman, Department of Health & Human Services (HHS) and FPKIPA Chair, called the meeting to order at 9:45 a.m. with attendee introductions.

The vote on the July 12, 2005 FPKIPA meeting minutes was postponed until members have had a chance to review/comment on the minutes. Members will submit their comments and vote to approve the minutes via email to Judith Fincher. These meeting minutes will be posted to the FPKIPA web site by COB 20 Sept. 2005.

Agenda Item 3

Electronic Mail Votes – Dr. Peter Alterman

The Wells Fargo Technical Interoperability Test Report and the Cross-certification of the Wells Fargo PKI at Basic Assurance with the FBCA was approved on 8-8-05 by 11 votes (or 85%), where 10 votes are required to achieve 75% approval. The Wells Fargo cross certification passes as of Monday, 8-8-05.

Approval vote of the Wells Fargo Technical Interoperability Test Report and Cross-Certification of Wells Fargo PKI at Basic Assurance with the FBCA			
Voting members	**Vote (Motion – DoD ; 2nd – Commerce)**		
	Yes	**No**	**Abstain**
Department of Commerce	X		
Department of Defense	X		
Department of Energy	X		
Department of Health & Human Services	X		
Department of Homeland Security	X		
Department of Justice	Absent-Did not Vote		
Department of State (proxy)	X		

Department of the Treasury	X		
GSA	X		
NASA	X		
OMB	Absent-Did not vote		
USDA/NFC	X		
USPTO	X		

ACTION: Mr. Brant Petrick will post the Cross-Certification of the Wells Fargo PKI at Basic Assurance with the FBCA to the web as of 8-8-05.

ACTION: Dr. Peter Alterman is to check to make sure he is on the right listserv (GSA), not Mitretek, because he has not been getting all the voting emails.

ACTION: Ms. Cheryl Jenkins will check on the status of the Wells Fargo MOA. We anticipate it soon.

Mapping of Boeing at Medium Assurance Level

The FPKIPA is waiting on two things from Boeing before we can vote to cross certify: 1) the audit report 2) the MOA. The vote on Boeing will come in October, at the earliest.

Dr. Alterman noted that the DoD ECA MOA has not been received yet.

ACTION: Mr. John Cornell will contact the DoD lawyer re the status of the DoD ECA MOA.

Dr. Alterman has received notice from the E-Authentication PMO that the Bank of America wants to cross certify with the Federal Bridge.

Agenda Item 4

Discussion/Vote on Draft Bylaws Document – Dr. Tice DeYoung

Dr. DeYoung and Mr. Froehlich drafted the "By-Laws and Operational Procedures and Practices of the Federal PKI Policy Authority" document. This document, with agreed revisions, was approved by over 75% of the voting members (see voting table below). The agreed revisions consist of 1) changing voting period from three to five days, 2) change "business days" to "working days," 3) incorporate all the changes Dr. Tice DeYoung has proposed in his email of August 4, 2005.

ACTION: Mr. Charles Froehlich was to clean up the By-Laws document, as agreed above, and send it to Mr. Brant Petrick for posting to the web site.

The By-laws revisions passed with 10 approval votes (77%), exceeding the 75% required.

Approval vote for FPKIPA By-laws			
Voting members	**Vote (Motion – Treasury ; 2nd – Commerce)**		
	Yes	**No**	**Abstain**
Department of Commerce	X		
Department of Defense	X		
Department of Energy	X		

Department of Health & Human Services	X		
Department of Homeland Security	Absent-Did not Vote		
Department of Justice	X		
Department of State	X		
Department of the Treasury	X		
GSA	Absent-Did not Vote		
NASA	X		
OMB	Absent-Did not Vote		
USDA/NFC	X		
USPTO	X		

ACTION: Mr. David Hanko, Ms. Cheryl Jenkins and Dr. Tice DeYoung were to define "emergency" as used in the By-Laws. Once resolved, the By-Laws would be modified and reposted to the web site.

The "Federal PKI Policy Authority Charter for Operations" was also discussed and it was decided to make changes to bring it into alignment with the By-Laws document, so that both documents agree with each other. The vote on the FPKIPA Charter was postponed until the September 13, 2005 meeting to allow members to review/comment on the revisions being undertaken by Ms. Cheryl Jenkins, who will also incorporate Dr. DeYoung's Charter-related comments (email of Aug. 4, 2005).

ACTION: Ms Cheryl Jenkins will scrub the Charter document to bring it into alignment with the By-Laws, change FBCA to Federal PKI architecture, and incorporate Dr. DeYoung's Aug. 4 comments on the Charter. This revised document will be circulated 5 days prior to the September 13, 2005 meeting.

Agenda Item 5

Discussion of Audit Cycle Review Issues – Ms. Cheryl Jenkins and Mr. Dave Hanko

Ms. Cheryl Jenkins is proposing that the audit cycle requirements be changed to a 3-phase cycle: 1) a full-blown audit the first year, 2) to be followed by a partial compliance audit for the next two years (against a checklist), 3) return to a full audit in the fourth year, i.e., would do an audit every three years. This would require changes to the MOAs and to the FBCA CP.

During the two intervening years agencies would perform an independent review against a checklist developed by the Policy Authority.

The checklist is based on the "top 20" most common errors found during Mr. Dave Hanko's analysis of 9 random audit reports. Ms Cheryl Jenkins is using Mr. Hanko's skeleton list to map each common error to federal security and FBCA policy requirements.

This could take the form of a self-assessment, although the use of an independent third party compliance review is the consensus of the Policy Authority. Ms. Jenkins stated that the checklist provides us with the 'flavor' of non-federal PKI's we're interoperating with.

Ms. Michelle Moldenhauer noted that Treasury will most likely do full compliance audits annually. It is likely that NFC will also perform annual audits because they're an SSP.

ACTION: Ms. Jenkins will refine the checklist developed by Mr. Hanko and will submit it to the CPWG for review/action. The checklist needs to be completed before it is emailed to the FPKIPA members. Ms Jenkins and Mr. Hanko are to keep Ms Kathy Sharp in the loop during this phase.

ACTION: Dr. Peter Alterman will present the "top 20" proposal to the CPWG on Aug. 30, 2005. A completed proposal is needed before the FPKIPA members vote on modifying the audit review requirements in the FBCA CP.

Agenda Item 6

Discussion: New FBCA Policy Update – NO VOTE - Mr. Tim Polk

The new FBCA CP (RFC 3647 format) was emailed to the FPKIPA members for review and comments and was posted (Draft version) to the FPKIPA web site.

ACTION: Mr. Tim Polk will send a summary of significant changes between RFC 3647 and RFC 2527 to the listserv.

ACTION: Mr. Brant Petrick is to forward an email from Ms. Judy Spencer on the changes to the FBCA CP (3647) to Dr. Peter Alterman.

ACTION: Mr. Tim Polk will draft a White Paper before the September 13 FPKIPA meeting, to be distributed after the policy is finished and voted. Agencies need to know the "gap" between RFC 2527 and RFC 3647, since agencies will be required to re-write their CP's.

ACTION: Ms Cheryl Jenkins will help Mr. Polk create a delta matrix table for agencies to use to measure their CP's.

These actions affect FY 2007 budgets.

Agenda Item 7

FPKI Certificate Policy Working Group (CPWG) Reports – Mr. Tim Polk

Mr. Brant Petrick mapped the new DoD CP (RFC 3647 format) against the new FBCA CP (RFC 3647 format) using the general requirements mapping matrix and the high level of assurance mapping matrix. The DoD general requirements mapping matrix was reviewed at the FPKI CPWG meeting on July 28, 2005. The CPWG stopped at item No.62 (of 130 mapping items), and Mr. Polk commented the mapping is "in good shape." .We will continue our review of the DoD 3647 mapping matrix at the Aug. 30, 2005, when Mr. Hanko can be present.

ACTION: Mr. Polk is to provide the changes for the Common Policy CP High Level of Assurance and get it into compliance with FIPS 201, as one change proposal to the FPKIPA listserv.

The vote on the Common Policy High will occur at the September 13, 2005 FPKIPA meeting.

ACTION: Ms. Jenkins is to add Mr. David Cooper to the GSA-maintained FPKIPA listserv.

ACTION: Mr. David Cooper is revising the Common Policy Certificate Profile for the SSP program to show what certificates and CRL's look like and will distribute it to the FPKIPA listserv at least 5 working days before the Sept. 13, 2005 FPKIPA meeting.

ACTION: Mr. Tim Polk is to send a memo to Dr. Peter Alterman from the CPWG recommending that Boeing be mapped at the Medium Assurance level.

The Vote to Map Boeing at Medium Assurance Level will be conducted via email.

ACTION: Ms Judy Fincher is to send Mr. Polk a separate list of his action items.

Agenda Item 8

FPKI Operational Authority (FPKI OA) Report – Ms. Cheryl Jenkins

Requirement for maintenance of test environments

Ms. Jenkins appealed to the members to stand up and make available a testing environment that mirrors their production environments, so that

1) We can advance the architecture
2) Do other kinds of testing.

The level of effort and cost factors for such a limited testing environment would be "significantly reduced: because

1) Testing would only occur 3 to 5 times per year
2) No crypto hardware is required.

Thus far, only ACES DST has done testing with Ms. Jenkins.

It was pointed out that NASA, DOE and USPTO maintain offline test environments.

ACTION: Ms. Jenkins will check with DOE and USPTO re using their test labs.

ACTION: Dr. Peter Alterman urged all members to respond to Ms. Jenkins with
I can do it and it will cost "X"
I cannot do it because….

Status of FBCA/Applicant Cross-Certification Technical Testing (changes in bold)

Completed			**Current**	**Future**
Dept of the Treasury	Dept of Energy	USPTO	**DOJ**	**Boeing**
NASA	State of Illinois	DHS		
USDA/NFC	Dept of Labor	HEBCA		
DoD	ACES/DST	Wells Fargo		
DoD KMI	ACES/ORC	**GPO**		
Government of Canada				
DoD ECA				
Dept of State	ACES/AT&T			

Ms. Jenkins stated we are "on schedule" in stabilizing the architecture. We are not in compliance with the Common Policy CP and are currently using the Microsoft Windows 2003 Server for the Common Policy CA. If the problem cannot be resolved in the next few days, the FPKI OA Team will swap with

the Cybertrust CA. If this is the result, the FPKI OA Team will have to re-issue certificates to all SSP's.

The architecture requires that everyone point their directories to the FPKI directory and everyone except Treasury has agreed that the FPKI directory is the superior directory.

ACTION: Ms Michelle Moldenhauer will coordinate a meeting with key persons and Treasury to address this.

Accreditation Update: FPKI A residual issues in the Hot Site are being taken care of this month. We will need to re-issue certificates to ACES/DST and USPTO due to erroneous information in the certificates. Since Mitreteck is R&D, a contract will be let out to manage operations for the FPKI architecture. September 30, 2006, is the targeted date to move the FPKI operations to a commercially managed service.

Dr. Alterman noted Ms Sarbari Gupta at Electrosoft Services is doing a study to determine where the physical FPKI Architecture should be located.

Ms. Jenkins provided an update on the progress of completing the Microsoft application to get the Common Policy root certificate into the Microsoft certificate store. This will cost us nothing. The application has 40 pages of Web Trust requirements in which the FPKI OA Team must map to their independent audit requirements.

ACTION: Dr. Alterman noted that we have an audience large (i.e., nationally and internationally) enough for Microsoft to approve it. Dr. Alterman and Ms. Jenkins will meet two weeks from now to review and modify the application's draft narrative language that will be used to prove that the FPKI audience is large enough.

Agenda Item 9

Other topics?

Ms. Moldenhauer raised the issue about whether or not the Treasury SSP (pending) has to be subordinate to the Common Policy Root CA.

Mr. Tim Polk commented: "If the user is using the Common Policy Root as the trust anchor, they can get to any Common Policy certificate issued by an SSP, e.g., Treasury."

ACTION: Ms. Jenkins, Mr. Polk and Ms. Moldenhauer are meeting 8-11-05 at noon at NIST to work through this issue [whether Treasury has to be subordinate to the Common Policy root CA].

ACTION: Ms. Jenkins is to send Dr. Alterman an email requesting a POC at Netscape. Dr. Alterman has a POC for Mozilla.

The next FPKIPA Meeting is scheduled for Sept. 13, 2005 (9:30 AM to 12:00 PM) at the GSA Central Office Building located at 1800 F Street, Room # 5141A, Washington, DC.

Agenda Item 10

Adjourn Meeting
The meeting adjourned at noon.

D. CURRENT ACTION ITEMS

No.	Action Statement	POC	Start Date	Target Date	Status
057	Write a short paper that says from here forward the FBCA OA will limit FBCA acceptance testing to systems that demonstrate enhanced assurance through NIAP testing.	Tim Polk, NIST	8 July 2003 Updated – 9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
062	Define the NIAP certification requirement for future bridge membrane applications.	Tim Polk, NIST	9 Sept 2003	9 Dec 2003 FPKIPA meeting	**Open**
085	Test/evaluate the PKCS-12 usage issue and make a recommendation to the FPKIPA at a meeting in the near future.	Tim Polk, NIST	13 July 2004	12 October 2004 FPKIPA meeting	**Open**
096	Research and draft FPKIPA charter updates to address Bridge-to-Bridge Cross-Certification.	Dr. Tice DeYoung, NASA	12 Oct 2004	Jan 2005 FPKIPA meeting	**Done**
097	Research and draft FBCA Criteria & Methodology document updates to address Bridge-to-Bridge Cross-Certification.	Dr. Peter Alterman, HHS	12 Oct 2004	Jan 2005 FPKIPA meeting	**Done**
112	Update their MOA with the FBCA to reflect the new one-way certificate being issue for the period of January 2005 to January 2006.	DoD	11 Jan 2005	28 Feb 2005	**Open**
113	Prepare and route a new Letter of Authorization from the FPKIPA to the FPKI OA for this new one-way cross-certificate for the DoD PKI for the period of January 2005 to January 2006.	John Cornell	11 Jan 2005	31 Jan 2005	**Open**
131	Develop a Compliance Audit Report paper on this issue and report to the FPKIPA at the 14 June FPKIPA meeting.	Cheryl Jenkins, GSA Dave Hanko, DoD	12 Apr 2005	14 June 2005 FPKIPA meeting	**Open**
132	The FBCA TWG will be tasked with determining the LOE and cost necessary to post the Common Policy CA certificate in the root store cache leading email vendor products and report their findings at a future FPKIPA meeting.	Cheryl Jenkins, GSA	12 Apr 2005	14 June 2005 FPKIPA meeting	**Done**

No.	Action Statement	POC	Start Date	Target Date	Status
133	All FPKIPA members contact FPKI OA re: cost and feasibility of limited testing environment.	All FPKIPA members	9 August 2005	11 October 2005	**Open**